UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/655,372	09/05/2003	Masanao Sakai	053969-0157	8586

22428 7590 04/29/2011

FOLEY AND LARDNER LLP
SUITE 500
3000 K STREET NW
WASHINGTON, DC 20007

EXAMINER	
PAN, JOSEPH T	
ART UNIT	PAPER NUMBER
2492	

MAIL DATE	DELIVERY MODE
04/29/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/655,372	SAKAI, MASANAO	
	Examiner	Art Unit	
	JOSEPH PAN	2492	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 March 2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,4,7,8,10,11,15,17,21,23,24,28-30 and 33-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,4,7,8,10,11,15,17,21,23,24,28-30 and 33-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office Action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 22, 2011 has been entered.

2. Applicant's response filed on October 22, 2010 has been fully considered. Claims 1, 8, 15, 21, and 30. Claims 5, 6, 12, 13, 18, 20, 25, 26, and 32 have been canceled. Claims 1, 3-4, 7-8, 10-11, 15, 17, 21, 23-24, 28-30, and 33-36 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 3-4, 7-8, 10-11, 21, 23-24, 28-30, and 33-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow et al. (U.S. Patent No. 6,175,917 B1), hereinafter "Arrow", in view of Sullenberger et al. (U.S. Patent No. 7,447,901 B1),

hereinafter "Sullengerger", and further in view of Bisbee et al. (U.S. Patent No. 7,657,531 B2), hereinafter "Bisbee".

Referring to claim 1:

i. Arrow teaches:

A network comprising:

IP processing apparatuses, which use an IP (Internet Protocol) for encrypting and authenticating communications via the Internet between two different centers (see figure 1, elements 115, 125, 135, 145, 155; and column 6, line 61, through column 7, line 7, of Arrow); and

an IP setting apparatus, which manages IP settings of the IP processing apparatuses (see figure 1, element 160 'VPN management station'; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15, of Arrow);

wherein in response to receiving a request from a first IP processing apparatus to communicate with a second IP processing apparatus, the second IP processing apparatus transmits a response (see column 7, lines 26-45, of Arrow);

wherein said IP setting apparatus generates SA (Security Association) parameters, to be used in the IP communication between the first and the second IP processing apparatuses, based on the contents of the request message and contents of IP policies stored by the IP setting apparatus (see figure 13, 1310 'define VPN parameters [i.e., generating Security Association (SA) parameters]', 1314 'define access control rules [i.e., generating IP policies]', of Arrow);

wherein said IP setting apparatus sends a distribution message including the policies of said IP and the SA parameters in response to the request message (see column 12, lines 22-25 'manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160', of Arrow).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

Arrow discloses that the VPN management unit issues a request to a VPN unit for configuration (see column 12, lines 22-25 'configuration module 710 of operating system 116 manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160.', of Arrow, emphasis added). Arrow further discloses that the VPN unit sends a request message to the VPN management unit (see column 12, line 25 'it also reports configuration status information concerning host VPN unit 115 to VPN management station 160', of Arrow). However, Arrow does not specifically mention that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit.

Arrow discloses that the IP setting apparatus transmits encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses (see column 11, lines 27-34, of Arrow). However, Arrow does not explicitly disclose the common encryption key.

Arrow does not explicitly disclose IPsec processing apparatus retransmits the request for communication to the IPsec setting apparatus and receives new setting information before a term of validity for the SA expires.

ii. Sullenberger teaches a method for establishing a dynamic multipoint encryption virtual private network, wherein Sullenberger that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit to dynamically establish an encrypted virtual private network (see figure 1; column 7, line 63 to column 8, line 3; and column 10, lines 38-51, of Sullenberger).

Sullenberger further discloses the IPsec protocol (see column 1, lines 50-59, of Sullenberger), the common encryption key (see column 2, lines 24-29; and column 7, lines 44-47, of Sullenberger), and the specific key lifetime values (see coumn 7, line 46, of Sullengerger).

On the hand, Bisbee teaches a method for state-less authentication, wherein Bisbee discloses IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires (see column 11, lines 1-7 'The Security Context and the symmetric session encryption key contained therein are then forwarded to the User and retained for the period for which the Security Context is valid. In some instances, the Time-Offset and Expiration Time values may also be returned to the User, which allows the User to **renew** the Security Context prior to its **expiration** [i.e., IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires].', of Bisbee)..

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sullenberger into the system of Arrow such that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit and dynamically establish an encrypted virtual private network, because Arrow teaches "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100." (see column 6, lines 31-34, of Arrow, emphasis added). Sullenberger teaches "The invention relates more specifically to a method and apparatus for establishing a **dynamic** multipoint encrypted virtual private network (VPN)." (see column 1, lines 19-21, of Sullenberger, emphasis added). Therefore, Sullenberger's teaching could enhance Arrow's system.

The ordinary skilled person would have been motivated to have applied the teaching of Bisbee into the system of Arrow such that a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires, because Arrow teaches defining Security Associations (SA) for a VPN unit (see figure 13, 1310 'define VPN parameters', of Arrow). Therefore, Bisbee's teaching could increase the network security for Arrow's system, because Bisbee requires a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires.

Referring to claims 3-4, 10-11, 16, 23-24, 29:

Arrow, Sullenberger, and Bisbee teach the claimed subject matter: a network (see claim 1 above). They further disclose transmitting messages between IPsec setting server apparatus and IPsec processing apparatus (see column 9, lines 19-22 of Arrow).

Referring to claim 7:

Arrow, Sullenberger, and Bisbee teach the claimed subject matter: a network (see claim 1 above). They further disclose the keys for encryption and authentication (see column 11, lines 32-34 of Arrow).

Referring to claim 8:

i. Arrow teaches:

An IP setting apparatus managing IP setting of IP processing apparatuses, which use an IP (Internet Protocol) for securing communication via the Internet between two different centers (see figure 1, element 160; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15, of Arrow),

wherein said IP setting apparatus manages IP policies applied among IP processing apparatus(see figure 1, element 160; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15 of Arrow);

wherein said IP setting apparatus includes means for specifying the IP policies of said IP to be applied between a first IP processing apparatus and the second IP processing apparatus (see figure 11, element 1102 'receive request to configure VPN unit'; figure 13, elements 1310 'define VPN parameters [i.e., Security Association (SA)', 1314 'define access control rules', 1316 'define address translation rules'; and column 15, line 52-column 16, line 15, of Arrow, emphasis added).
wherein said IP setting apparatus generates SA (Security Association) parameters, to be used in the IP communication between the first and the second IP processing apparatuses, based on the contents of the request message and contents of IP policies stored by the IP setting apparatus (see figure 13, 1310 'define VPN parameters [i.e.,

generating Security Association (SA) parameters]', 1314 'define access control rules [i.e., generating IP policies]', of Arrow); and

wherein said IP setting apparatus sends a distribution message including the policies of said IP and the SA parameters in response to the request message (see column 12, lines 22-25 'manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160', of Arrow).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

Arrow discloses that the VPN management unit issues a request to a VPN unit for configuration (see column 12, lines 22-25 'configuration module 710 of operating system 116 manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160.', of Arrow, emphasis added). Arrow further discloses that the VPN unit sends a request message to the VPN management unit (see column 12, line 25 'it also reports configuration status information concerning host VPN unit 115 to VPN management station 160', of Arrow). However, Arrow does not specifically mention that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit.

Arrow discloses that the IP setting apparatus transmits encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses (see column 11, lines 27-34, of Arrow). However, Arrow does not explicitly disclose the common encryption key.

Arrow does not explicitly disclose IPsec processing apparatus retransmits the request for communication to the IPsec setting apparatus and receives new setting information before a term of validity for the SA expires.

ii. Sullenberger teaches a method for establishing a dynamic multipoint encryption virtual private network, wherein Sullenberger that a VPN unit makes a request to the VPN management unit in order to communicate with another

VPN unit to dynamically establish an encrypted virtual private network (see figure 1; column 7, line 63 to column 8, line 3; and column 10, lines 38-51, of Sullenberger).

Sullenberger further discloses the IPsec protocol (see column 1, lines 50-59, of Sullenberger), the common encryption key (see column 2, lines 24-29; and column 7, lines 44-47, of Sullenberger), and the specific key lifetime values (see coumn 7, line 46, of Sullengerger).

On the hand, Bisbee teaches a method for state-less authentication, wherein Bisbee discloses IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires (see column 11, lines 1-7 'The Security Context and the symmetric session encryption key contained therein are then forwarded to the User and retained for the period for which the Security Context is valid. In some instances, the Time-Offset and Expiration Time values may also be returned to the User, which allows the User to **renew** the Security Context prior to its **expiration** [i.e., IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires].', of Bisbee)..

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sullenberger into the system of Arrow such that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit and dynamically establish an encrypted virtual private network, because Arrow teaches "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100." (see column 6, lines 31-34, of Arrow, emphasis added). Sullenberger teaches "The invention relates more specifically to a method and apparatus for establishing a **dynamic** multipoint encrypted virtual private network (VPN)." (see column 1, lines 19-21, of Sullenberger, emphasis added). Therefore, Sullenberger's teaching could enhance Arrow's system.

The ordinary skilled person would have been motivated to have applied the teaching of Bisbee into the system of Arrow such that a VPN unit

retransmitts a request to the VPN management unit before a term of validity for the SA expires, because Arrow teaches defining Security Associations (SA) for a VPN unit (see figure 13, 1310 'define VPN parameters', of Arrow). Therefore, Bisbee's teaching could increase the network security for Arrow's system, because Bisbee requires a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires.

Referring to claim 30:

Arrow, Sullenberger, and Bisbee teach the claimed subject matter: an IPsec processing apparatus (see claim 15 above). They further disclose the SPD [i.e., Security Policy Database], SAD [i.e., Security Association Database] (see figure 2, elements 203 'IPSec Policy', 124C 'security association', of Sullenberger).

Referring to claim 21:

i. Arrow teaches:

An IPsec setting method comprising:

receiving from IP processing apparatus a request (see column 14, lines 33-44, of Arrow),

retrieving IP policy rules from memory and generating IP settings parameters based on the content of the request from the IP processing apparatus and the retrieved policy rules (see column 14, lines 33-44, of Arrow); and

transmitting the generated IP settings to the IP processing apparatus (see column 14, lines 33-44, of Arrow),

wherein said IP setting apparatus generates SA (Security Association) parameters, to be used in the IP communication between the first and the second IP processing apparatuses, based on the contents of the request message and contents of IP policies stored by the IP setting apparatus (see figure 13, 1310 'define VPN parameters [i.e., generating Security Association (SA) parameters]', 1314 'define access control rules [i.e., generating IP policies]', of Arrow);

wherein said IP setting apparatus sends a distribution message including the policies of said IP and the SA parameters in response to the request message (see column 12, lines 22-25 'manages the configuration of VPN unit 115 in

response to configuration requests or commands from VPN management station 160', of Arrow).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

Arrow discloses that the VPN management unit issues a request to a VPN unit for configuration (see column 12, lines 22-25 'configuration module 710 of operating system 116 manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160.', of Arrow, emphasis added). Arrow further discloses that the VPN unit sends a request message to the VPN management unit (see column 12, line 25 'it also reports configuration status information concerning host VPN unit 115 to VPN management station 160', of Arrow). However, Arrow does not specifically mention that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit.

Arrow discloses that the IP setting apparatus transmits encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses (see column 11, lines 27-34, of Arrow). However, Arrow does not explicitly disclose the common encryption key.

Arrow does not explicitly disclose IPsec processing apparatus retransmits the request for communication to the IPsec setting apparatus and receives new setting information before a term of validity for the SA expires.

ii. Sullenberger teaches a method for establishing a dynamic multipoint encryption virtual private network, wherein Sullenberger that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit to dynamically establish an encrypted virtual private network (see figure 1; column 7, line 63 to column 8, line 3; and column 10, lines 38-51, of Sullenberger).

Sullenberger further discloses the IPsec protocol (see column 1, lines 50-59, of Sullenberger), the common encryption key (see column 2, lines 24-29;

and column 7, lines 44-47, of Sullenberger), and the specific key lifetime values (see coumn 7, line 46, of Sullengerger).

On the hand, Bisbee teaches a method for state-less authentication, wherein Bisbee discloses IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires (see column 11, lines 1-7 'The Security Context and the symmetric session encryption key contained therein are then forwarded to the User and retained for the period for which the Security Context is valid. In some instances, the Time-Offset and Expiration Time values may also be returned to the User, which allows the User to **renew** the Security Context prior to its **expiration** [i.e., IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires].', of Bisbee)..

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sullenberger into the system of Arrow such that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit and dynamically establish an encrypted virtual private network, because Arrow teaches "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100." (see column 6, lines 31-34, of Arrow, emphasis added). Sullenberger teaches "The invention relates more specifically to a method and apparatus for establishing a **dynamic** multipoint encrypted virtual private network (VPN)." (see column 1, lines 19-21, of Sullenberger, emphasis added). Therefore, Sullenberger's teaching could enhance Arrow's system.

The ordinary skilled person would have been motivated to have applied the teaching of Bisbee into the system of Arrow such that a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires, because Arrow teaches defining Security Associations (SA) for a VPN unit (see figure 13, 1310 'define VPN parameters', of Arrow). Therefore, Bisbee's teaching could increase the network security for Arrow's system, because Bisbee requires a VPN unit

retransmitts a request to the VPN management unit before a term of validity for the SA expires.

Referring to claim 28:

Arrow, Sullenberger, and Bisbee teach the claimed subject matter: an IPsec setting method (see claim 21 above). They further disclose the inquiry means (see column 14, line 25, of Arrow).

Referring to claims 33-35:

Arrow, Sullenberger, and Bisbee teach the claimed subject matter: a network (see claim 1 above). They further discloses transmitting the encryption key to the first and the second IPsec processing apparatus depending on their addresses (see column 9, lines 18-22, of Arrow), and the common encrypt key (see column 2, lines 24-29; and column 7, lines 44-47, of Sullenberger).

Referring to claim 36:

Arrow, Sullenberger, and Bisbee teach the claimed subject matter: a network (see claim 1 above). They further discloses the encrypted communication (see column 11, lines 43-45, of Arrow).

4. Claims 15, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow et al. (U.S. Patent No. 6,175,917 B1), in view of Sullenberger et al. (U.S. Patent No. 7,447,901 B1), further in view of Bisbee et al. (U.S. Patent No. 7,657,531 B2), and further in view of Park et al. (U.S. Pub. No. 2003/0126466 A1).

Referring to claim 15:

i. Arrow teaches:

An IP processing apparatus using an IP (Internet Protocol) on the Internet,

wherein said IP processing apparatus receives from an IP setting apparatus managing communication a packet containing the IP to be applied to communication with another IP processing apparatus, determines whether or not to

request from the IP setting apparatus a setting for IP communication (see column 4, lines 38-40; column 11, lines 27-30 of Arrow), and

wherein the IP processing apparatus transmits a request to the IP setting apparatus in order to receive from the IP setting apparatus a setting for IP communication (see figure 11, element 1102 'receive request to configure VPN unit'; figure 13, elements 1310 'define VPN parameters', 1314 'define access control rules', 1316 'define address translation rules'; and column 15, line 52-column 16, line 15, of Arrow, emphasis added),

wherein said IP processing apparatus includes means for setting an SPD (Security Processing Database), in which policies for applying said IP is recorded, and an SAD (Security Association Database), in which an SA (security Association) necessary for subjecting an individual communication to the IP processing is stored, based upon a message received from the IP setting apparatus (see column 13, lines 60-64 'database 906 [i.e., SPD/SAD]; and figure 13, 1310 'define VPN parameters [i.e., generating Security Association (SA) parameters]', 1314 'define access control rules [i.e., generating IP policies]', of Arrow);

wherein said IP setting apparatus sends a distribution message including the policies of said IP and the SA parameters in response to the request message (see column 12, lines 22-25 'manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160', of Arrow).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

Arrow discloses that the VPN management unit issues a request to a VPN unit for configuration (see column 12, lines 22-25 'configuration module 710 of operating system 116 manages the configuration of VPN unit 115 in response to configuration requests or commands from VPN management station 160.', of Arrow, emphasis added). Arrow further discloses that the VPN unit sends a request message to the VPN management unit (see column 12, line 25 'it also reports configuration status

information concerning host VPN unit 115 to VPN management station 160', of Arrow). However, Arrow does not specifically mention that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit.

Arrow discloses that the IP setting apparatus transmits encryption keys to the first and second IP process apparatuses to be used to encrypt and authenticate IP communications between the first and second process apparatuses (see column 11, lines 27-34, of Arrow). However, Arrow does not explicitly disclose the common encryption key.

Arrow does not explicitly disclose IPsec processing apparatus retransmits the request for communication to the IPsec setting apparatus and receives new setting information before a term of validity for the SA expires.

Arrow discloses the database. However, Arrow does not explicitly disclose the SPD (Security Processing Database) and SAD (Security Association Database).

ii. Sullenberger teaches a method for establishing a dynamic multipoint encryption virtual private network, wherein Sullenberger that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit to dynamically establish an encrypted virtual private network (see figure 1; column 7, line 63 to column 8, line 3; and column 10, lines 38-51, of Sullenberger).

Sullenberger further discloses the IPsec protocol (see column 1, lines 50-59, of Sullenberger), the common encryption key (see column 2, lines 24-29; and column 7, lines 44-47, of Sullenberger), and the specific key lifetime values (see coumn 7, line 46, of Sullengerger).

On the hand, Bisbee teaches a method for state-less authentication, wherein Bisbee discloses IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires (see column 11, lines 1-7 'The Security Context and the symmetric session encryption key contained therein are then forwarded to the User and retained for the period for which the Security Context is valid. In some instances, the Time-Offset and Expiration Time values may also be returned to

the User, which allows the User to **renew** the Security Context prior to its **expiration** [i.e., IP processing apparatus retransmits the request for communication to the IP setting apparatus and receives new setting information before a term of validity for the SA expires].', of Bisbee).

On the other hand, Park teaches a method for controlling an internet information security system in an IP packet level, wherein Park discloses the SPD (Security Processing Database) and SAD (Security Association Database) (see page 2, [0034] 'SPD' 'SAD', of Park)

iii. The ordinary skilled person would have been motivated to have applied the teaching of Sullenberger into the system of Arrow such that a VPN unit makes a request to the VPN management unit in order to communicate with another VPN unit and dynamically establish an encrypted virtual private network, because Arrow teaches "VPN management station 160 controls VPN units 115, 125 and 135 through commands and configuration information transmitted to the respective VPN unit through public network 100." (see column 6, lines 31-34, of Arrow, emphasis added). Sullenberger teaches "The invention relates more specifically to a method and apparatus for establishing a **dynamic** multipoint encrypted virtual private network (VPN)." (see column 1, lines 19-21, of Sullenberger, emphasis added). Therefore, Sullenberger's teaching could enhance Arrow's system.

The ordinary skilled person would have been motivated to have applied the teaching of Bisbee into the system of Arrow such that a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires, because Arrow teaches defining Security Associations (SA) for a VPN unit (see figure 13, 1310 'define VPN parameters', of Arrow). Therefore, Bisbee's teaching could increase the network security for Arrow's system, because Bisbee requires a VPN unit retransmitts a request to the VPN management unit before a term of validity for the SA expires.

The ordinary skilled person would have been motivated to have applied the teaching of Park into the system of Arrow to include a SPD and SAD, because Arrow teaches defining Security Associations (SA) for a VPN unit using

database which includes information reflecting the structure of virtual private networks supported by the system and the configuration of the VPN units supported by the VPN management station (see column 13, lines 60-64, of Arrow). Therefore, Park's teaching could enhance Arrow's system by including SPD and SAD for defining Security Associations (SA).

Referring to claim 17:

Arrow, Sullenberger, Bisbee, and Park teach the claimed subject matter: an IPsec setting method (see claim 21 above). They further disclose the IPsec processing apparatus receiving a message from an IPsec setting apparatus, and transmits a request for communicating with another IPsec processing to the IPsec setting apparatus (see e.g. figure 8, 818 'create security context and provide to user', 820 'submit request for access and security context', of Bisbee).

Response to Arguments

5. Applicant's arguments, filed on October 22, 2010, have been fully considered. The independent claims 1, 8, 15, and 21 have been amended to include the new limitation "wherein the IPsec processing apparatus retransmits the request for communication to the IPsec setting apparatus and receives new setting information before a term of validity for the SA expires.". Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is being made in view of Bisbee.

(a) Applicant argues:

"In contrast, in the present invention as claimed, the IKE is not used for acquisition of the common encryption key. Rather, the IPsec setting apparatus "generates SA (Security Association) parameters, to be used in the IPsec communication between the first and the second IPsec processing apparatuses,"

without the use of the IKE, to supply IPsec processing apparatuses with the SA parameter." (see page 11, 2nd paragraph).

Examiner matinains:

The primary reference Arrow teaches "In state 1310, the system manager defines VPN parameters [i.e., the system manager generate parameters to be used in the IP communication between the first and the second IP processing apparatuses without the use of the IKE] for authentication, encryption [i.e., the encryption key], and compression functions to be associated with a newly created VPN." (see column 15, lines 52-54, of Arrow). Therefore, Arrow discloses generates SA (Security Association) parameters, to be used in the IP communication between the first and the second IP processing apparatuses," without the use of the IKE, to supply IP processing apparatuses with the SA parameter. Arrow discloses the IP protocol. However, Arrow does not discloses the IPsec protocol.

On the other hand, Sullenberger discloses the IPsec protocol (see column 1, line 50 'IPsec protocol', of Sullenberger).

Therefore, the combination of the references disclose generates SA (Security Association) parameters, to be used in the IPsec communication between the first and the second IPsec processing apparatuses," without the use of the IKE, to supply IPsec processing apparatuses with the SA parameter, such as claimed.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached at 571-272-4006. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Joseph Pan/

Examiner, Art Unit 2492

April 26, 2011

/saleh najjar/

Supervisory Patent Examiner, Art Unit 2492